TANÚSÍTVÁNY FELÜLVIZSGÁLATI Jegyzőkönyv

A **HUNGUARD** Számítástechnikai-, informatikai kutató-fejlesztő és általános szolgáltató Kft. a 9/2005. (VII.21.) IHM rendelet alapján, mint a Magyar Köztársaság Miniszterelnöki Hivatalt Vezető Miniszterének 001/2010 számú Kijelölési okiratával kijelölt tanúsító szervezet és mint a NAT által NAT-6-0048/2011 számon akkreditált terméktanúsító szervezet

Tanúsítvány felülvizsgálati eljárás keretében
megvizsgálta
a **HUNG-T-054-2010 TANÚSÍTVÁNYBAN**
foglaltakat, és annak tartalmát összevetette az NMHH által kibocsátott EF-26838-8/2011, EF-26838-9/2011, EF-26838-10/2011, EF-26838-11/2011, EF-26838-12/2011, EF-26838-13/2011 határozataiban foglalt új követelményekkel.

Megállapítja, hogy:
a **nCipher Corporation Ltd**. által fejlesztett

nShield F3 Ultrasign PCI /Hw: nC4033P-300/
nShield F3 Ultrasign 32 PCI, /Hw: nC4132P-300/
nCipher F3 PCI for NetHSM, /Hw: nC4032P-300N/
payShield Ultra PCI Hw: /nC4232P-300/
payShield Ultra PCI for NetHSM /Hw: nC4232P-300N/
nShield F3 PCI /Hw: nC4032P-150/
payShield PCI, és /Hw: nC4232P-150/
nShield Lite, /Hw: nC4032P-10/
förmver verzió: 2.22.6-3

elektronikus aláírási termék

hitelesítés szolgáltatatásra való felhasználási feltételei az alábbiakban módosul

1. SHA-1 vagy annál gyengébb lenyomatoló algoritmus használata 2012 január 1-e után tilos
2. RSA aláírási algoritmus használata esetén a minimális modulus ajánlott mérete (MinModLen) 2048 bit
3. DSA aláírási algoritmus használata esetén az ajánlott minimális p prímhosszúság (pMinLen) 2048 bit, a minimális q prímhosszúság (qMinLen) 224 bit

A Tanúsítvány Felülvizsgálati Jegyzőkönyv regisztrációs száma: **HUNG-FJ-054/1-2011**
Kelt: Budapest, 2011. december 15.

PH.

Endrődi Zsolt
Tanúsítási igazgató

dr. Szabó István
Ügyvezető igazgató